UNITED STATES DISTRICT COURT

for the

District of Guam

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Dropbox accounts associated with llarmawhl@gmail.com and llarmawhal2@gmail.com that are stored at premises owned by Dropbox, Inc. (See Attachment A)

Case No. MJ-23-00056

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Dropbox accounts associated with llarmawhl@gmail.com and llarmawhal2@gmail.com that are stored at premises owned by Dropbox, Inc. Property is further described in Attachment A.

located in the _____ District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Sections 2252 and 2252A	Certain activities relating to material involving the sexual exploitation of minors and Certain activities relating to material constituting or containing child pornography

The application is based on these facts:

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

STEVEN CAVITT, Special Agent, HSI
Printed name and title

BP

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 5/5/23

Judge's signature

City and state: Hagatna, Guam

HON. MICHAEL J. BORDALLO, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Steven Cavitt, being duly sworn, depose and state that the following is true to the best of my information, knowledge, and belief:

A. Introduction and Agent Background

1. I am a Special Agent with United States Immigration and Customs Enforcement, Homeland Security Investigations (HSI), and I am authorized to conduct investigations into violations of Federal law including: the smuggling of narcotics, weapons, and various types of contraband; financial crime and export enforcement issues; cybercrime; child exploitation; immigration crime; human rights violations; human trafficking and smuggling, national security, and gang investigations. I have been employed with HSI since January 14, 2008. Prior to employment with HSI, I was employed as a police officer in Wichita, Kansas from 1997 to 2008.

2. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of Title 18, United States Code, Sections 2251, 2252, and 2252A. I have received training and instruction in the field of investigation of child pornography and have had the opportunity to participate in investigations relating to the sexual exploitation of children. As part of my training and experience, I have reviewed images containing child pornography in a variety of formats (such as digital still images and video images) and media (such as digital storage devices, the Internet, and printed images).

3. This affidavit is submitted in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., an electronic communications service/remote computing service provider headquartered in San Francisco, California. The information to be searched

relates to accounts associated with email addresses llarmawhal@gmail.com and llarmawhal2@gmail.com and is more particularly described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Dropbox, Inc., to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

These email addresses are linked to Andrew Taylor WOOD, an active-duty United States Navy member, currently stationed on Guam, There is probable cause to believe that located in the places described in Attachment A are items described in Attachment B, being evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252(a)(1), (2), and (4) and 2252A(a)(1), (2), (3), and (5).

4. This Court previously issued a search warrant, MJ-23-00040 for information stored by Dropbox, Inc., related to the same accounts. While reviewing the return from Dropbox for that warrant, agents noticed that certain information was not included. After correspondence with Dropbox, agents concluded that the best course of action was to obtain a second warrant with additional language in Attachment B identifying the missing information which constitutes evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252(a)(1), (2), and (4) and 2252A(a)(1), (2), (3), and (5). This affidavit is thus submitted in order to more specifically describe the information sought in Attachment B.

5. Specifically, agents seek the upload dates and times and information related to sharing of electronic files associated with the accounts above and stored by Dropbox, Inc, as described in Attachment B.

6. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A are located in the place described in Attachment A.

7. The information contained within the affidavit is based on my training and experience, as well as information imparted to me by other law enforcement officers involved in this investigation.

B. Relevant Statutes

8. This investigation concerns alleged violations of 18 U.S.C. Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors.

9. 18 U.S.C. Sections 2252 and 2252A prohibit a person from knowingly possessing or accessing sexually explicit images (child pornography) with the intent to view them as well as transporting, receiving, distributing, or possessing in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, any visual depiction of minors engaging in sexually explicit conduct (child pornography).

C. Jurisdiction

10. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

D. Definitions

11. The following definitions apply to this Affidavit.

12. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

13. "Visual depictions" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image See 18 U.S.C. § 2256(5).

E. CyberTipline Reports

14. The National Center for Missing and Exploited Children ("NCMEC") is an organization that, among other things, tracks missing and exploited children and serves as a repository for information about child pornography. Federal law requires NCMEC to operate the CyberTipline and requires Electronic Service Providers to report apparent instances of child pornography offenses. Providers also have the discretion to submit reports concerning planned or imminent child pornography offenses. Companies that suspect child pornography has been stored or transmitted on their systems report that information to NCMEC in a CyberTipline Report (or "CyberTip"). The Electronic Service Provider submits the report and uploads content to NCMEC via a secure connection. Aside from required information such as incident type, date, and time, reporters can also fill in voluntary reporting fields such as user or account information, IP addresses, or information regarding the uploaded content itself, as well as other information it may have collected in connection with the suspected criminal activity. The Electronic Service Provider may or may not independently view the content of the file(s) it uploads. Using publicly available

search tools, NCMEC then attempts to locate where the activity occurred based on the information the Electronic Service Provider submits, such as IP addresses. NCMEC then packages the information from the Electronic Service Provider along with any additional information it has, such as previous related CyberTips, and sends it to law enforcement in the jurisdiction where the activity is believed to have occurred.

15. On July 15, 2020, the Electronic Service Provider Dropbox, Inc, ("ESP") submitted CyberTipline Report #74802689 to the National Center for Missing and Exploited Children ("NCMEC"). As reported by the ESP, the incident type was: Apparent Child Pornography, and the incident time was listed as: 07/14/2020, 20:34:16 UTC.

16. Dropbox is a service that allows its users to store files on Dropbox's servers. According to Dropbox's privacy policy, at https://www.dropbox.com/privacy, Dropbox collects and stores "the files you upload, download, or access with the Dropbox Service," and also collects logs: "When you use the Service, we automatically record information from your Device, its software, and your activity using the Services. This may include the Device's Internet Protocol ("IP") address, browser type, the web page visited before you came to our website, information you search for on our website, locale preferences, identification numbers associated with your Devices, your mobile carrier, date and time stamps associated with transactions, system configuration information, metadata concerning your Files, and other interactions with the Service. , "Dropbox is a free service that lets you bring all your photos, docs, and videos anywhere. This means that any file you save to your Dropbox will automatically save to all your computers, phones and even the Dropbox website."

17. From my experience and information provided by the ESP, I know Dropbox to be a personal cloud storage service that allows users to store files online, making them accessible from

their computer, telephone, or tablet computing device. Once uploaded, files may be synced across multiple devices and may be shared with others.

18. The ESP also uploaded file(s) in connection with the report, the content of which NCMEC did review. The report indicated that the ESP reviewed the contents of the files. The ESP reported additional information including the following: IP addresses; screen name; username; email address, and multiple file names.

19. NCMEC then used publicly available search tools to discover that the IP address the ESP reported resolved to Hagatna and Barrigada, Guam.

20. I know from my training and experience that the ESP flags and reports images or files that have the same "hash values" as images that have been reviewed and identified by NCMEC or by law enforcement as child pornography. A hash value is akin to a fingerprint for a file. The contents of a file are processed through a cryptographic algorithm, and a unique numerical value – the hash value - is produced that identifies the unique contents of the file. If the contents are modified in any way, the value of the hash will also change significantly. I know from my training and experience that the chances of two files with different content having the same hash value are infinitesimal.

21. Here, I know from my training and experience that the ESP compares the hash values of files that its customers transmit on its systems against the list of hash values that NCMEC has. If the ESP finds that a hash value of a file on its systems matches one on the list, it captures the file along with information about the user who posted, possessed, or transmitted it on the ESP's systems.

22. Some CyberTipline Reports contain additional information about the type of child pornography that is depicted in the images and/or videos reviewed by the ESPs. This categorization

system was developed by various ESPs in January 2014. In terms of the content, a file that contains the letter "A" depicts a prepubescent minor and a file that contains the letter "B" depicts a pubescent minor. Further, a file that contains the number "1" depicts a "sex act," defined by the ESPs as "[a]ny image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person (sic) of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value". A file that contains the number "2" depicts "lascivious exhibition", defined by the ESPs as "[a]ny image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value". For example, a file with the description "A1" has been designated by an individual to depict a prepubescent minor engaged in a sex act. CyberTipline Report #74802689 contains images with the following classifications: A1 (302 instances); A2 (38 instances); B1 (20 instances); and B2 (9 instances).

23. CyberTipline Report #74802689 also provided basic subscriber information maintained by the ESP. The associated username was "Andrew Worthson" and the email address was llarmawhal@gmail.com (identified as having been verified on 28 March 2016). Four Internet Protocol (IP) addresses were listed as having been used to log into the account: 202.151.68.47 (a Teleguam Holdings, LLC, IP address, used on 16 January 2020); 103.7.101.12 (a Teleguam Holdings, LLC, IP address, used on 22 January 2020); 209.164.184.192 (a Level 3 Communications/Teleguam Holdings, LLC, IP address, used on 11 May 2020); and 202.128.68.51 (a Docomo Pacific Guam IP address, used on 12 July 2020).

24. On 28 October 2022, Naval Criminal Investigative Service (NCIS) Special Agent Robert Frasco and I conducted a preliminary review of the data stored within CyberTipline Report #74802689. During this preliminary review, Special Agent Frasco and I determined the vast majority of the reviewed media unambiguously depicted minors involved in sexual activity or lascivious exhibition. Additionally, various files were explicitly titled to indicate sexual content involving minors. Such file titles included: "Pthc Pedo – 11Yo & 13Yo Girls Play With Mom's Pussy And Fuck Dad).avi", "Boy & girl.avi", "hornytoad's best cp ptn lsm pthc (121).jpg", ""pthc_10yo_Beauty_Preteen_Blowjob-Anal-Cumshot.3gp", "torture_4_lolitacity (58).jpg", "14yo British girl.mp4".

F. Identification of Andrew Taylor WOOD

25. On 20 April 2022, I received the results of a subpoena served upon Google. According to Google, email account llarmawhal@gmail.com is associated with Google Account ID: 600418679173 and was created on 22 March 2012. The user's name for the account "taylor WOOD". An account recovery email address of phantomfirez2@gmail.com and telephone number +1 (619) 980-5623 were listed. Customer information from the account identified a Payments Profile (created on 18 December 2018), with two billing addresses: Andrew WOOD, Ballston Spa, NY 12020, and Andrew WOOD, GU. A linked Visa card with billing information of Andrew WOOD, Ballston Spa, NY 12020, was also noted. Based on Special Agent Frasco's experience with the United States Navy's submarine forces, I learned there is a Nuclear Power Training Unit, in Ballston Spa, NY. It is a training location for personnel assigned to work with nuclear reactors.

26. On 20 April 2022, I received the results of a subpoena served upon GTA Teleguam regarding the IP addresses listed in CyberTipline Report #74802689. According to GTA, on 16 January 2020, IP address 202.151.68.47 was associated with subscriber Andrew Taylor WOOD

with related telephone number (671) 482-5247. His service address was listed as #3 Chapel Road Barracks RM 205B, Santa Rita GU 96915 and his email address was jrspyingeyes@gmail.com. The account was activated on 03 February 2019. The information provided for IP address 103.7.101.12 on 22 January 2020 also indicated Andrew Taylor WOOD with the same information as above. The IP address 209.164.184.192 was associated with GTA's cellular tower switches, for which users are not logged.

27. On 21 April 2022 and 22 April 2022, Special Agent Frasco queried various Department of Defense (DoD) databases to identify information regarding Andrew Taylor WOOD. According to the DoD Person Search database (which retains basic biographical identifiers, addresses, telephone numbers, and email addresses for service members, DoD employees, and dependents), Andrew Taylor WOOD, with date of birth 04 May 1998, is assigned to USS KEY WEST (SSN 722), has telephone (671) 482-5247 listed as his home number. His address was listed as 3 Chapel Rd, #305B, Santa Rita, GU. Special Agent Frasco also reviewed data from the Defense Biometric Identification System (DBIDS), which confirmed Andrew Taylor WOOD has current and routine access to Naval Base Guam. Checks of additional DoD systems revealed Andrew Taylor WOOD is an enlisted Electronics Technician Nuclear, which Special Agent Frasco knows to be a Navy rating tasked with maintaining electronics systems related to nuclear reactors aboard aircraft carriers and submarines. SA Frasco further knows the USS KEY WEST to be a nuclear-powered fast-attack submarine based at Naval Base Guam.

28. On 04 May 2022, I received the results of a subpoena served to Docomo Pacific regarding IP address 202.128.68.51. According to Docomo Pacific, this IP address (used on 12 July 2020) is used for Docomo's public Wi-Fi services offered for Military Lodging customers at Andersen Air Force Base and Naval Base Guam.

29. On 23 November 2022, Special Agent Frasco contacted Kevin Kay, the Asset Protection and Safety Manager for Navy Exchange (NEX) on Guam. Kay confirmed that Wi-Fi at Andersen Gateway Inns and Suites (aboard Andersen Air Force Base) and Navy Gateway Inns and Suites (aboard Naval Base Guam) is provided by Docomo Pacific.

30. On 25 November 2022, Special Agent Frasco met with April Zapatos, Unaccompanied Housing manager at Naval Base Guam. Zapatos confirmed "Andrew WOOD", a Sailor from USS KEY WEST, was assigned to Building 3, Room 205B, and had resided there since 04 February 2019. The telephone number listed for him was (671) 482-5247. Zapatos further verified that both Docomo Pacific and GTA provide internet access to Barracks 3 and individual residents may choose which provider they wish to use. However, Unaccompanied Housing does not keep records regarding which provider residents use.

G. SEIZURE OF DEVICES AND ACCOUNTS ASSOCIATIONS WITH WOOD

31. On 29 November 2022, myself and Special Agent Frasco interviewed Andrew Taylor WOOD. WOOD provided extensive background regarding his internet access, his use of digital devices, and his consumption of pornography. WOOD advised that, in 2020, he used GTA internet in his barracks and never shared access to his router with any other individual. WOOD acknowledged using the email address llarmawhal@gmail.com primarily to access pornography and to moving pornographic material between various computers, devices, and external storage drives. WOOD further confirmed his use of the email addresses phantomfirez2@gmail.com and jrspyingeyes@gmail.com. WOOD denied ever having viewed child pornography. Upon being confronted about connections between himself and child pornography, WOOD requested a lawyer, terminating the interview.

32. On 29 November 2022, NCIS and HSI agents seized Andrew Taylor WOOD's cellular telephone and conducted a search of his barracks room pursuant to a federal search warrant. This search resulted in the seizure of several digital devices capable of accessing the internet. Specifically, and relevant to this affidavit, agents seized

(A) One Musetex desktop computer tower.
(B) A Samsung Tablet, Model SM-Y290, S/N: RNWMB136CFJ.
(C) A white Oculus virtual reality headset with controllers.
(D) A Microsoft Surface 4 laptop, Model 1951, S/N: 043160710457.
(E) A Kindle, Model PQ94WIF.
(F) An MSI gaming series laptop, Model: MS-1655, black with red logo.
(G) A Samsung Galaxy S8, Model: SM-G950U, IMEI: 355986083898594.
(H) A Nintendo Switch with inserted memory card (SD 512 GB Micro XC (Switch)).
(I) A Nintendo Wii S/N: LU541705913.
(J) XBOX 360 (black), S/N: 120569510808.
(K) An Acer Aspire laptop 5250-BZ669, S/N: LXRJY021031410F60E1601.
(L) A Samsung Galaxy S5 cell phone, IMEI: 354691063545576 with SIM card inserted.
(M) Samsung Galaxy S7 Edge, IMEI: 357216073382971, damaged, with black/grey Pelican case (broken).
(N) Samsung cellular telephone bearing IMEI: 355602111089854, in a black and gray case.

33. Between 02 December 2022 and 05 December 2022, NCIS analyst Derek Paoletti and Special Agent Frasco conducted internet searches for the email address llarmawhal@gmail.com and the username "llarmawhal". These searches identified numerous social medial accounts, community forum postings, and online profiles. Multiple social media accounts with the username "llarmawhal" identify the user as "Taylor WOOD" or "Taylor", display his correct date of birth, or correspond with his known location at the time of the depicted activity. Two posts by a user by the name "llarmawhal" on a sex-themed community forum (Sexingforum.net) indicate the user was searching to trade pornographic material via Kik Messenger account "llarmawhal". In one such post, dated 15 October 2016, titled "Young Dropbox Group Active", the user states "I am making a db/videos/pic trading group for active members only". In a second such post, dated 28 August 2019, the user stated "I'm looking for boys with sisters. I'll make it worth your while if you

can fulfill my requests, I have plenty to trade" and again referenced the same Kik account. One website (booru.allthefallen.moe) with username "llarmawhal" listed as a registered user is dedicated to the sharing of animated depictions of children (including toddlers and babies) in sexual contexts. Several of the identified profiles indicate the user was last active shortly before NCIS and HSI seized WOOD's devices on 29 November 2022.

34. On 02 December 2022, Special Agent Frasco sent a preservation letter to Kik/MediaLab regarding the account "llarmawhal". Kik/MediaLab responded the following day, advising that account was banned on 31 August 2021 with no data retained.

35. On December 14, 2022 and January 12, 2023, HSI Special Agent Mike Lansangan and I reviewed three of the devices seized from WOOD pursuant the federal search warrant on November 29, 2022. Special Agent Lansangan identified at least 15 user accounts associated with the email address llarmawhal@gmail.com saved on WOOD's Samsung Galaxy cellular telephone bearing IMEI 355602111089854. Notable accounts include:

Website	**Creation Date**	**Email/Username**
Kiksexting.com	10 September 2018	llarmawhal@gmail.com
Dropbox.com	09 February 2022	llarmawhal2@gmail.com
Dropbox.com	03 December 2017	llarmawhal@gmail.com
Allthefallen.moe	11 December 2021	llarmawhal@gmail.com

36. Special Agent Lansangan further identified that the Samsung Galaxy S8 cellular telephone application data revealed "Dropbox Cloud Storage" version 200.2.10 was purchased/installed on 16 July 2020. Web history results on this device identified the user accessed Dropbox.com via the user email address llarmawhal@gmail.com on 11 May 2020 (UTC) and 12

July 2020 (UTC). These dates and approximate times correspond to two of the logins noted in the original CyberTip. Additionally, Special Agent Lansangan's examination of the Musetex desktop computer identified user data indicating the computer's user had accessed www.dropbox.com."

37. On January 12, 2023, Special Agent Cavitt sent preservation requests to Dropbox and Google for all records relating to llarmawhal2@gmail.com. Additionally, Special Agent Cavitt previously sent a preservation request to Google and Dropbox for llarmawhal@gmail.com. Dropbox responded reference llarmwhal@gmail.com, that they had no records to produce because our request was outside of the original 90-day preservation period.

38. On 17 January 2023, NCIS Analyst Paoletti conducted additional internet research regarding accounts known, or believed to be, associated with Andrew Taylor WOOD. Paoletti identified numerous additional posts on Sexingforum.net and the similarly-themed KikSexting.com that were either from the username "llarmawhal" or referenced a Kik username "llarmawhal". Combined, these posts revealed the same user was evidently associated with the Kik usernames "llarmawhal", "scantrell69", and "sexysynthiacantrell". Examples of such posts include:

- On 20 December 2016, a Sexingforum.net post titled "Looking To Start A Dropbox Trade Group" by "llarmawhal" contained the message "Send me a link or vid if you are interested in joining. I don't much care what the vid is off, no topics are really taboo. KIK: llarmawhal".

- On 14 January 2017, a Sexingforum.net post titled "Dropbox Trade Group" by "llarmawhal" contained the message "I have a Dropbox trading group that has open spots. Send a taboo link, any type, to join. Kik is llarmawhal".

- On 13 March 2017, a Sexingforum.net post titled "Dropbox Trade Group" by "llarmawhal" contained the message "Looking to start another Dropbox trade group. No limits. Kik at llarmawhal if you are interested. Just send something to be added.".

- On 18 October 2017, a Sexingforum.net post titled "Dropbox Trade" by "llarmawhal" contained the message "Hey, i'm looking to trade taboo dropbox, i have a bit of everything. Let me know what you are into and send at least a pic and i'll send back. Kik: llarmawhal".

- On 31 August 2021, a KikSexting.com post titled "Taboo" by user "Spoopy Ghost" contained the message "Hi, I'm looking to trade some taboo. Send something of the type you want back. If you are F, you can send nudes and I will send links back. Kik is llarmawhal".

- On 01 September 2021, a KikSexting.com post titled "23f Looking For Taboo" by user "Spoopy Ghost" contained the message "I'm trading nudes for taboo links. If you don't send a link first, I'm not going to reply. I can also trade links if you prefer that. Kik is scantrell69".

- 20 November 2022, a KikSexting.com post titled "Taboo" by user "Spoopy Ghost" contained the message "Trading nudes for taboo links. Send link in first message or i will not respond. I don't have time to waste on people that don't have anything. My KIK is sexysynthiacantrell".

Additionally, a nearly identical username in Sexingforum.net, "llarmawhals", also posted various messages between 18 January 2017 and 22 January 2017, which identified the user as a 17-year-old female looking to trade "live pics" with other females and identified their Kik username as "llarmawhal".

39. Also on 17 January 2023, given the evident association between the usernames "llarmawhal" and the username "SexySynthiaCantrel" (or variations), Paoletti conducted further searches of the KikSexing.com and Sextingforum.net websites for additional possibly associated users. Paoletti identified a post by SexySynthiaCantrel, dated 18 October 2017, titled "Highschool Girl Trading Nudes ;)" in which the user wrote "Hit me up boys, i'm selling nudes for cheap I can prove I'm real Kik: SexySynthiaCantrel".

40. On February 8, 2023, a second federal search warrant was obtained for an expanded digital forensic examination of digital devices seized on November 29, 2022. On February 16, 2023, Special Agents Cavitt, Frasco, and Lansangan further reviewed three of the devices. On WOOD's Samsung Galaxy cellular telephone bearing IMEI 355602111089854, Agents located additional accounts associated to llarmawhal, and llarmawhal2@gmail.com. Notable accounts include:

Website	**Creation Date**	**Email / Username**
My.plcoud.com	30 April 2017	Larmawhal2@gmail.com
Sextingforum.net	28 August 2019	Llarmawhal
unknown	unknown	Username: SexySynthiaCantrell User ID: Sexysynthiacantrell_7ef@talk.kik.com User Profile Photo- associated to llarmawhal2@gmail.com
https://imgsrc.ru/	13 September 2017	llarmawhal

41. SA Cavitt has learned through training and experience from other agents that https://imgsrc.ru/ is a Russian based photo sharing website that is known for being used for the trading of child exploitation material. Open-source research advised the following: Imgsrc is a free photo sharing website based in Russia. The site allows users to post images of any content,

and some members have used the website to spread child pornography. A few of the website's users have been arrested and charged under criminal law. Most of the site operates legally. (www.reference.com).

H. Digital Media

42. Based on my training and experience in the investigation of child pornography, and information related to me by other law enforcement officers involved in the investigation of child pornography, I know digital devices include cellular telephones, tablets, email devices, and personal digital assistants, which usually provide internet and cellular network access. Digital media devices are capable of storing content and data including, but not limited to, numbers (phone numbers and names associated with those numbers), text (in the form of text messages, personal reminders, etc.), picture files (jpeg, gif, bmp, dib, jpg, etc.), music files (midi, wav, mp3, mp4, etc.), movie files (mpg, mpeg, aif, mov, ram, etc.), web history and application data, and any other data capable of being stored on a digital communications device or accompanying removable media; all of which can be reasonably expected to be seized from the digital communication device. Based on my training and experience, individuals who use social networking sites often do so using multiple digital media platforms and a variety of software applications. These include, but are not limited to, social networking websites/applications, internet message boards/forums, and photo/video sharing webpages.

43. I also know many electronic devices have cellular and internet capabilities. Due to these technological advancements, electronic devices that possess cellular and internet features are able to use mobile Wi-Fi hotspots. Mobile hotspot capability allows for wireless data from a cellular provider to be utilized to provide internet access to other devices such as cellular devices, computers, tablets, and other Wi-Fi enabled devices. I know connecting a laptop or other device

to a mobile hotspot will result in a cellular service provider IP address. The specific IP address used by a given device if often retained within application databases or activity logs on the device, providing a link between a given device and a specific IP address long after the date of the internet activity.

44. Based on my experience and information from the application's public website, I know Kik Messenger to be a chat application that allows users to communicate via text and video call and exchange media. Users may create accounts with minimal personal information and may search for other users by username or find new users by searching for groups of common interest. From my experience with this application, numerous chat groups on Kik (which may be entered freely by any user) have themes relating to illicit sexual activity, including incest, bestiality, and underage activity.

I. Child Exploitation and the Internet

45. Based on previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who possess, access with intent to view, or collect, trade, and/or disseminate child pornography.

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, videos, books, drawings, or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own

sexual arousal and gratification. Such individuals prefer not to be without their child pornography for prolonged periods of time. This behavior has been documented by law enforcement officers involved in investigations of child pornography throughout the world.

c. Such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer, smart telephone, and surrounding area, often storing copies on multiple devices or in multiple locations. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis; however, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

d. Internet websites, social media applications, forums, and online chat communities provide such individuals with the opportunity to find other individuals with similar predilections in order to obtain new media to satiate their desire for child pornographic images. Individuals may trade for like images (exchanging child pornography for child pornography) or may provide other content of interest (such as adult pornography, fetish-themed pornography, or animated depictions of child sexual activity) in exchange for child pornography.

e. Such individuals, in corresponding with others with similar desires or while searching for such trading partners, often use coded phrases to reference or indicate an interest or openness to such content. Such phrases include, but are not limited to, "taboo", "no limits", "pervy", "loli", "shota", or "jail bait". They may also refer to peripheral topics, such as incest or "family nudism", as these topics by their very nature may involve children.

J. Conclusion

46. Based on the investigation described above, probable cause exists to believe that the Dropbox, Inc accounts, usernames/emails llarmawhal@gmail.com and llarmawhal2@gmail.com, linked to Andrew Taylor WOOD, likely contain evidence of the receipt, possession, viewing, and distribution of child pornography. At least three of the seized devices contain data associated with the Dropbox account, found to contain child pornography in July 2020. Internet activity between 2016 and 2022 for the username "llarmawhal" (and associated usernames and social media handles) reveals WOOD has actively sought to collect and trade "young", "taboo", "no limits", and incest-themed media via both Dropbox and Kik. The first such observed activity was in October 2016 most recent such activity was in November 2022, suggesting WOOD is a long-term collector and/or trader of such media, with the behavior continuing to the present. Consequently, it is probable each of the Dropbox accounts in Attachment A contains a) child pornographic media; b) digital artifacts associating WOOD with Dropbox, Kik, or various known (and potentially hitherto unidentified) websites and forums; or c) communications (including via social media, online forums/groups, or telephone) with other individuals for the purpose of discussing, obtaining, trading, or distributing child pornography. Any such data would constitute evidence, fruits, and instrumentalities of a violation of Title 18, United States Code, Sections 2252(a)(1), (2), (4) and 2252A(a)(1), (2), (3), and (5).

47. As noted in Section A above, on March 24, 2023, the District Court of Guam issued search warrant MJ-23-00040, which was served on Dropbox on March 25, 2023. Dropbox complied on April 6, 2023. While reviewing the provided information, agents noticed Dropbox had not provided upload dates and times and information related to sharing of files. Your affiant inquired to Dropbox who replied in part: "Dropbox may have available a list of shared links created by the requested account, and a log of timestamps relating to uploads within an account. If you wish to request either of these data points, they must be clearly and specifically requested within the search warrant document."

48. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the subject accounts, described in Attachment A for the items listed in Attachment B, with additional language added related to the above-referenced correspondence with Dropbox.

49. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

50. The government will execute this warrant by serving the warrant on Dropbox, Inc. Because the warrant will be served on Dropbox, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

I declare under penalty of perjury that the foregoing is true and correct to the best of my information, knowledge, and belief.

_____

Steven Cavitt, Special Agent
Homeland Security Investigations

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

This warrant applies to information associated with Dropbox accounts associated with llarmawhal@gmail.com (User Identification Number 364283682) and llarmawhal2@gmail.com (unknown User Identification Number) that are stored at premises owned, maintained, controlled or operated by Dropbox, Inc. ("Dropbox"), an electronic service provider that accepts service of legal process at 333 Brannan Street, San Francisco, CA 94107.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Dropbox (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit card or bank account numbers);

b. The types of service utilized;

c. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

d. All records pertaining to communications between Dropbox, Inc., and any person regarding the account, including contacts with support services and records of actions taken;

e. All user content created, uploaded, or shared by the account;

f. All images and videos in the account;

g. All shared links created by the account; and

h. Log of timestamps relating to uploads within the account(s).

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252A; those violations involving user or users of each account or identifier listed in Attachment A, including information pertaining to the following matters:

a. the production, distribution, receipt, or possession of images of child pornography or images of obscene material; or correspondence in furtherance of the commission of offenses involving the production, distribution, receipt or possession of child pornography or obscene material.

b. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

c. All images depicting children engaging in sexually explicit conduct as defined in 18 U.S.C. § 2256.

III. Method of delivery

Dropbox shall disclose items seized pursuant to this search warrant by sending (notwithstanding Title 18, United States Code, Section 2252A, or similar statute or code) to the listed Special Agent. Dropbox shall disclose responsive data, if any, by delivering on any digital media device via Federal Express c/o Special Agent Steve Cavitt, DHS-ICE-HSI, 291 Chalan Pasaheru, Suite 200, Tamuning, Guam 96913.